

**Garantia de la Informació i Seguretat****2013/2014**

Codi: 102757

Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502441 Enginyeria Informàtica	OT	4	2

**Professor de contacte**

Nom: Guillermo Navarro Arribas

Correu electrònic: Guillermo.Navarro@uab.cat

**Utilització d'idiomes**

Llengua vehicular majoritària: català (cat)

Algun grup íntegre en anglès: No

Algun grup íntegre en català: Sí

Algun grup íntegre en espanyol: Sí

**Prerequisits**

No hi ha requisits oficials, però sí es recomana tenir coneixements bàsics sobre criptografia, xarxes i programació. Aquests coneixements són assolibles amb assignatures prèvies del grau: Xarxes, Informació i Seguretat i Metodologia de la Programació.

**Objectius**

Aquesta és una assignatura que mostra aspectes generals sobre la seguretat de la informació. Es dóna una visió global sobre punts clau de seguretat informàtica que comprenen des de la seguretat en xarxes i Internet, fins al *malware* o virus.

L'objectiu d'aquesta assignatura és que l'alumne assoleixi uns coneixements bàsics sobre la problemàtica de la seguretat de la informació i els mecanismes existents per a la protecció de sistemes informàtics. D'aquesta manera, l'alumne pot desenvolupar una visió crítica envers la seguretat informàtica. Per altra banda els alumnes hauran de ser capaços de posar en pràctica alguns aspectes de l'assignatura. Conèixer com es realitzen certs atacs és un pas important per entendre les necessitats de seguretat dels sistemes, i poder després aplicar tècniques de protecció adequades en cada cas.

**Competències**

- Enginyeria Informàtica
- Adquirir hàbits de pensament
- Adquirir hàbits de treball personal.
- Capacitat per a comprendre i aplicar els principis de l'avaluació de riscos i aplicar-los correctament a l'elaboració i execució de plans d'actuació
- Capacitat per a comprendre, aplicar i gestionar la garantia i seguretat dels sistemes informàtics
- Capacitat per a determinar els requisits dels sistemes d'informació i comunicació d'una organització atenent a aspectes de seguretat i compliment de la normativa i la legislació vigent.
- Capacitat per dissenyar, desenvolupar, avaluar i assegurar l'accessibilitat, l'ergonomia, la usabilitat i la seguretat dels sistemes, serveis i aplicacions informàtiques, així com de la informació que gestionen
- Concebre i desenvolupar sistemes o arquitectures informàtiques centralitzades o distribuïdes integrant hardware, software i xarxes
- Treballar en equip

**Resultats d'aprenentatge**

1. Col·laborar en el disseny i seguiment de les polítiques de seguretat de sistemes informàtics.
2. Comprendre i aplicar els principis de seguretat a l'elaboració i execució de plans d'actuació.
3. Conèixer els principis de la informàtica forense i del tractament dels delictes informàtics.
4. Conèixer i comprendre les possibilitats tècniques d'implantació de polítiques de seguretat en sistemes distribuïts.
5. Desenvolupar la capacitat d'anàlisi, síntesi i prospectiva.
6. Determinar els requisits de seguretat i compliment de la normativa i la legislació vigent en els sistemes d'informació i comunicació d'una organització.
7. Determinar els requisits de seguretat i confidencialitat, així com identificar els principals tipus d'atacs i amenaces.
8. Dissenyar sistemes de protecció de la informació: control d'accés i integritat.
9. Treballar cooperativament.
10. Treballar de manera autònoma.

## Continguts

1. Introducció a la seguretat i gestió de vulnerabilitats
  1. Propietats de seguretat
  2. Gestió de vulnerabilitats
  3. Models d'anàlisi d'amenaces
2. Mecanismes de seguretat
  1. Mecanismes d'autenticació
  2. Mecanismes d'autorització i control d'accés
  3. Mecanismes de seguretat en xarxes
  4. Detecció de malware i virus
  5. Sistemes de detecció d'intrusions
3. Gestió de la seguretat
  1. Gestió de riscos
  2. Polítiques de seguretat
  3. Informàtica forense i pericial
  4. Enginyeria social

El contingut de l'assignatura queda dividit en 3 blocs. El primer consta d'una introducció on es mostra la problemàtica de la seguretat informàtica: què és, com es classifica i com es mesura una vulnerabilitat de seguretat; com i qui gestiona les vulnerabilitats i amenaces de seguretat, etc. Tot seguit, el segon bloc, que és el bloc principal de l'assignatura, detalla mecanismes de seguretat concrets. Aquí es veuran diversos aspectes rellevants de la seguretat informàtica, per exemple com són el virus i com funciona un sistema antivirus; quins atacs es poden donar en xarxes d'ordinadors i quins mecanismes tenim per a la seva protecció; mecanismes d'autenticació com ara password i SSO, etc. Finalment, hi ha una tercera part sobre la gestió de la seguretat on es veuran aspectes addicionals com la informàtica pericial o l'enginyeria social.

## Metodologia

L'assignatura es desenvolupa en 50 hores d'activitats dirigides repartides en sessions de teoria, de problemes i de laboratori. En el plantejament de l'assignatura es potenciarà el treball tutoritzat sobre aspectes concrets de l'assignatura. Aquest treball es divideix en una part supervisada que es realitzarà a les sessions (de teoria, problemes i laboratori), i un treball no supervisat que l'alumne realitzarà de manera autònoma.

- Classes magistrals: classes realitzades a les sessions de teoria on el professor subministrarà informació sobre els coneixements de l'assignatura i sobre estratègies per adquirir, ampliar i organitzar aquests coneixements.
- Treball supervisat: el professor planteja uns problemes o activitats que els alumnes hauran de desenvolupar en grup. Aquest treball consta d'una part de treball supervisat i una part de treball autònom. La part supervisada es repartirà en sessions de problemes, teoria i laboratori, on els alumnes treballaran amb l'ajuda i guia del professor. Això comprèn des de la resolució de problemes a la realització de pràctiques al laboratori. Els treballs s'aniran plantejant al llarg del curs i la seva realització serà majoritàriament en grup.

## Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Sessions de laboratori	12	0,48	1, 2, 3, 4, 5, 6, 7, 8, 9
Sessions de problemes	12	0,48	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Sessions de teoria	26	1,04	1, 2, 3, 4, 6, 7, 8
Tipus: Supervisades			
Treball tutoritzat	18	0,72	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Tipus: Autònomes			
Preparació i estudi pràctic	45	1,8	1, 2, 3, 4, 5, 6, 7, 8, 9
Preparació i estudi teòric	30	1,2	1, 2, 3, 4, 5, 6, 7, 8, 10

## Avaluació

L'avaluació es farà en base al seguiment de l'estudiant durant l'assignatura. Es divideix principalment en dos blocs:

- Avaluació individual: es divideix en evidències concretes sobre el contingut de l'assignatura i avaluació del treball supervisat de forma individual. Tot i que pot haver una part d'avaluació de caire pràctic, es tracta majoritàriament de treball teòric.
- Avaluació col·lectiva: consta majoritàriament de l'avaluació del treball supervisat tant a nivell teòric com pràctic.

Com es pot veure, les activitats d'avaluació es divideixen en proves individuals i col·lectives tant de caire pràctic com de caire teòric. Les proves individuals es duran a terme al llarg del curs de forma continuada. Tot i així es preveu la realització d'una prova final que permeti recuperar les proves parcials d'avaluació individual.

Sobre l'avaluació continuada que es durà a terme durant el curs es preveu la realització de:

- 2 proves parcials d'avaluació individual.
- Avaluació del treball supervisat: cada treball supervisat serà avaluat tant de la part teòrica com de la part pràctica per separat. Aquesta avaluació pot ser tant col·lectiva com individual.

Per poder aprovar l'assignatura cal aprovar per separat cada part.

La qualificació de "no presentat" s'atorgarà als estudiants que no participin en una o més de les avaluacions, i que no n'hagin suspès cap altra (i.e., hagin obtingut una qualificació superior o igual a 5 sobre 10).

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, es qualificaran amb un zero les irregularitats comeses per l'estudiant que puguin conduir a una variació de la qualificació d'un acte d'avaluació. Per tant, copiar o deixar copiar una pràctica o qualsevol altra activitat d'avaluació implicarà suspendre-la amb un zero, i si és necessari superar-la per aprovar, tota l'assignatura quedarà suspesa. No seran recuperables les activitats d'avaluació qualificades d'aquesta forma i per aquest procediment, i per tant l'assignatura serà suspesa directament sense oportunitat de recuperar-la en el mateix curs.

Les dates d'avaluació continuada i lliurament de treballs es publicaran al campus virtual i poden estar subjectes a canvis de programació per motius d'adaptació a possibles incidències. Sempre s'informarà al campus virtual sobre aquests canvis ja que s'entén que el CV és el mecanisme habitual d'intercanvi d'informació entre professors i estudiants.

Es detallaran amb prou temps d'antelació els mecanismes d'avaluació, metodologia o funcionament general de

l'assignatura que no s'hagin concretat en aquesta guia.

## Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Proves individuals	40%	3	0,12	1, 2, 3, 4, 5, 6, 7, 8, 10
Treball pràctic	30%	2	0,08	1, 2, 3, 4, 5, 6, 7, 8, 9
Treball teòric	30%	2	0,08	1, 2, 3, 4, 5, 6, 7, 8, 9, 10

## Bibliografia

De manera orientativa es dona la següent bibliografia per a l'assignatura:

- Mark Stamp (2011) Information Security: principles and practice, 2n Edition. John Wiley & Sons.
- Ross Anderson (2008) Security Engineering. A Guide to Building Dependable Distributed Systems, Wiley, 2nd Edition.
- Matt Bishop (2002) Computer Security: Art and Science, Addison-Wesley.
- William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin (2003) Firewalls and Internet Security: Repelling the Wily Hacker. 2nd Edition, Addison-Wesley.
- Dieter Gollmann (2011) Computer Security, 3rd Edition. John Wiley & Sons
- Xabiel García Pañeda, David Melendi Palacio (2008) La peritación informática, un enfoque práctico, Colegio Oficial de Ingenieros en Informática Principado de Asturias.
- Stuart McClure, Joel Scambray, George Kurtz (2012) Hacking Exposed. Network Security Secrets & Solutions. McGraw-Hill Osborne Media, 7th edition.
- Peter Szor (2005) The Art of Computer Virus Research and Defense. Addison-Wesley.